

(19)日本特許庁 (JP) (12) 公開特許公報 (A) (11)特許出願公開番号
 特開2002-354048
 (P2002-354048A)

(43)公開日 平成14年12月6日 (2002.12.6)

(51) Int.Cl. ⁷	識別記号	F I	マークト [®] (参考)
H 04 L 12/66		H 04 L 12/66	A 5 K 0 3 0
12/46		12/46	A 5 K 0 3 3
			E
12/56	1 0 0	12/56	1 0 0 Z

審査請求 未請求 請求項の数 5 OL (全 7 頁)

(21)出願番号 特願2001-160311(P2001-160311)

(22)出願日 平成13年5月29日 (2001.5.29)

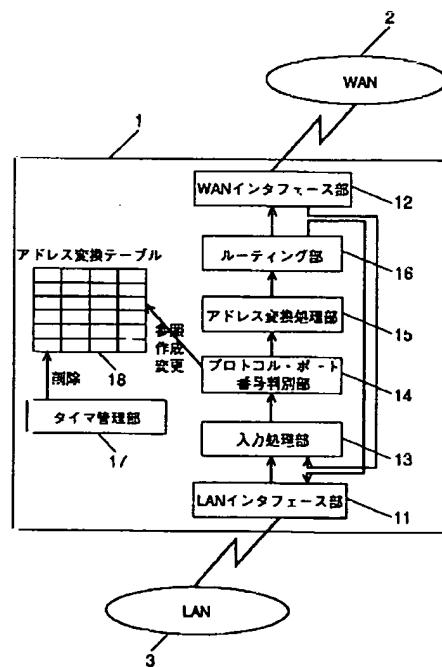
(71)出願人 000003821
 松下電器産業株式会社
 大阪府門真市大字門真1006番地
 (72)発明者 村川 泰
 大阪府門真市大字門真1006番地 松下電器
 産業株式会社内
 (72)発明者 原口 雅彦
 大阪府門真市大字門真1006番地 松下電器
 産業株式会社内
 (74)代理人 100097445
 弁理士 岩橋 文雄 (外2名)

最終頁に続く

(54)【発明の名称】 ルータ装置

(57)【要約】

【課題】 適切な通信接続性を確保し、効率的にメモリを利用可能としたルータ装置の提供を目的とする。
 【解決手段】 WAN 2と LAN 3との間に介在してアドレス変換を行うルータ装置 1において、一連の通信セッションを識別するプロトコル・ポート番号判別部 14 を備え、プロトコル・ポート番号判別部 14 は、アドレス変換テーブル内でアドレス変換エントリの関連付けを行い、エントリ生存時間を同期させるものとすることで、アドレス変換機能のために通信セッションが不正に切断されることを防ぎ、適切な通信接続性を確保し、効率的にメモリを利用して高速のアドレス変換エントリ管理方式を提供することができる。



【特許請求の範囲】

【請求項1】グローバルアドレスネットワークとプライベートアドレスネットワークの間に介在してアドレス変換を行うルータ装置において、一連の通信セッションを識別するプロトコル・ポート番号判別部を備え、同プロトコル・ポート番号判別部は、アドレス変換テーブル内でアドレス変換エントリの関連付けを行い、エントリ生存時間を同期させるものであることを特徴とするルータ装置。

【請求項2】前記プロトコル・ポート番号判別部は、前記一連の通信セッションと識別された複数のアドレス変換エントリをグループ化し、グループ毎で一括した操作を行うものであることを特徴とする請求項1記載のルータ装置。

【請求項3】前記プロトコル・ポート番号判別部は、アドレス変換エントリ生成時に、通信プロトコルの性質に応じて適切なエントリ生存時間を割り当てるものであることを特徴とする請求項1記載のルータ装置。

【請求項4】前記プロトコル・ポート番号判別部は、アドレス変換エントリ生成時に、通信相手先に応じて適切なエントリ生存時間を割り当てるものであることを特徴とする請求項1記載のルータ装置。

【請求項5】前記プロトコル・ポート番号判別部は、前記一連の通信セッションを監視し、端末間の通信状態を把握しながらエントリ生存時間を動的に変化させるものであることを特徴とする請求項1記載のルータ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、グローバルアドレスネットワークとプライベートアドレスネットワークとの間に介在してアドレス変換を行うルータ装置に関し、より詳しくは、ルータ装置におけるアドレス変換エントリ管理方式に関する。

【0002】

【従来の技術】近年、インターネットの爆発的普及に伴い、小規模なオフィス環境や家庭でも複数台のパーソナルコンピュータ（以下、「PC」と称す）などの端末をインターネットに接続する需要が高まっている。インターネットへの接続は、ローカルエリアネットワーク（以下、「LAN」と称す）を構築し、このLANに接続されたルータ装置を介して行うのが一般的である。

【0003】インターネットに接続するにはグローバルIPアドレスが必要となるが、これをLAN内の端末の台数分確保するのは非常に困難なので、通常LAN内ではプライベートIPアドレスを用いる。そして、インターネットを介して通信をする場合、ルータ装置上でNAT(Network Address Translation)やIPマスカレードと呼ばれるアドレス変換を行うことでインターネットへ接続する。

【0004】以下、従来のアドレス変換方式について説

明する。

【0005】図8は従来のネットワーク構成とアドレス変換処理の概要を示す図である。

【0006】図8において、PC101, 102, 103はLAN104に接続されている。ルータ装置105はLAN104とインターネット106との間に介在し、これらの間でアドレス変換を行う。また、インターネット106には端末107が接続されているものとする。なお、PC101のIPアドレスをA、ルータ装置105のインターネット106側のIPアドレスをB、端末107のIPアドレスをCとする。

【0007】PC101から端末107にパケットを送信する場合、送信元IPアドレスはA、宛先IPアドレスはCのパケットとなる。このパケットは、ルータ装置105によりインターネット106に向けてルーティングされるが、アドレス変換機能により送信元IPアドレスAがルータ装置105のインターネット106側のIPアドレスであるBに書き換えられる。このとき、ルータ装置105のアドレス変換テーブルには、この変換に関するアドレス変換エントリが追加され、以後、PC101と端末107の間で行われる同じプロトコルの通信に関してはこのアドレス変換エントリが参照されアドレス変換が行われる。また、ルータ装置105のメモリには容量の上限があるため、一定時間の参照のないアドレス変換エントリはテーブルから削除される。このアドレス変換機能により、プライベートアドレスで構築されるLAN104内の端末からインターネット106に接続することが可能になる。

【0008】

【発明が解決しようとする課題】しかしながら、上記従来の方式では、ルータ装置105はLAN104内からの接続のたびにアドレス変換エントリを生成し、このエントリが決めた規則に則ってアドレス変換を行うだけであり、各アドレス変換エントリ間の関係性を考慮していない。このため、アドレス変換テーブルのメモリ利用が効率的でなく、テーブル中のアドレス変換エントリの数が増えるにつれてエントリ検索に時間が掛かることになる。その結果、通信セッションが終了していないにも関わらず、エントリの生存時間切れと判定されて不当に通信セッションが切断されることも起こりうる。

【0009】ここで、図9を用いて上記従来の方式によるアドレス変換処理によって起こりうる問題について詳細に説明する。図9において、111はプライベートアドレスネットワーク内のPC、112はルータ装置、113はグローバルアドレスネットワーク内の端末である。ここでは、PC111がFTPクライアント、端末113がFTPサーバとなってFTP通信を行いう場合を考える。なお、PC111、ルータ装置112、端末113のIPアドレスをそれぞれA、B、Cとする。

【0010】FTP(File Transfer P

proto1) は、FTP通信の制御命令のやりとりをするFTP制御コネクション(TCPポート21番)と、実際にデータ転送を行うFTPデータコネクション(TCPポート20番)という2つのコネクションによりFTP通信を行う。PC111から端末113に対してFTP通信を行う場合、ルータ装置112がこれらの間に介在してアドレス変換を行う。ルータ装置112は、PC111からのパケットについては送信元IPアドレスをAからBに変換してから端末113に転送し、端末113からのパケットについては宛先IPアドレスをBからAに変換してPC111に転送する。

【0011】ここで、PC111が端末113から巨大なファイルをダウンロードする場合、FTPデータコネクションにおいてファイル転送をしている間、FTP制御コネクションの方には通信が発生しないため、このコネクションに関するルータ装置112内のアドレス変換エントリの生存時間が切れ、エントリが削除されてしまう。したがって、データ転送終了後にPC111から端末113にFTP制御命令を送ろうとしても、ルータ装置112は既にそれに対応したアドレス変換エントリを削除しているため新規にエントリを作成しなければならず、端末113において別セッションとみなされてパケット破棄され、FTP通信が正常に完遂できなくなる。

【0012】そこで、本発明では、適切な通信接続性を確保し、効率的にメモリを利用可能としたルータ装置を提供することを目的とする。

【0013】

【課題を解決するための手段】上記課題を解決するための本発明のルータ装置は、ルータ装置を通過する通信を監視し、アドレス変換テーブル内でアドレス変換エントリの関連付けを行い、エントリ生存時間を同期させるように構成したものである。

【0014】本発明のルータ装置によれば、適切な通信接続性を確保し、効率的にメモリを利用して高速のアドレス変換エントリ管理方式を提供することができる。

【0015】

【発明の実施の形態】請求項1に記載の発明は、グローバルアドレスネットワークとプライベートアドレスネットワークの間に介在してアドレス変換を行うルータ装置において、一連の通信セッションを識別するプロトコル・ポート番号判別部を備え、同プロトコル・ポート番号判別部は、アドレス変換テーブル内でアドレス変換エントリの関連付けを行い、エントリ生存時間を同期させることを特徴とするルータ装置であり、アドレス変換機能のために通信セッションが不正に切断されることを防ぐことができる。

【0016】請求項2に記載の発明は、プロトコル・ポート番号判別部は、一連の通信セッションと識別された複数のアドレス変換エントリをグループ化し、グループ毎で一括した操作を行うものであることを特徴とする請

求項1記載のルータ装置であり、アドレス変換テーブルにおけるメモリ利用を効率化し、グループ毎で一括した操作を行うことで、エントリ管理の簡易化、高速化が可能となる。

【0017】請求項3に記載の発明は、プロトコル・ポート番号判別部は、アドレス変換エントリ生成時に通信プロトコルの性質に応じて適切なエントリ生存時間を割り当てるものであることを特徴とする請求項1記載のルータ装置であり、アドレス変換機能のために通信セッションが不正に切断されることを防ぐことができ、効率的なメモリ利用が可能となる。

【0018】請求項4に記載の発明は、プロトコル・ポート番号判別部は、アドレス変換エントリ生成時に、通信相手先に応じて適切なエントリ生存時間を割り当てるものであることを特徴とする請求項1記載のルータ装置であり、アドレス変換機能の安全性を高めることができる。

【0019】請求項5に記載の発明は、プロトコル・ポート番号判別部は、一連の通信セッションを監視し、端末間の通信状態を把握しながらエントリ生存時間を動的に変化させるものであることを特徴とする請求項1記載のルータ装置であり、効率的なメモリ利用が可能となる。

【0020】以下、本発明の実施の形態について、図面を参照しながら説明する。

【0021】(実施の形態1) 図1は本発明の第1実施の形態におけるネットワーク構成を示す図である。第1実施の形態と従来の技術との相違点は、アドレス変換エントリを関連付け、その生存時間の同期を行うところにある。

【0022】図1において、本発明の第1実施の形態におけるルータ装置1は、グローバルアドレスネットワークとしてのインターネットなどのワイドエリアネットワーク(以下、「WAN」と称す)2と、プライベートアドレスネットワークとしてのLAN3との間に介在してアドレス変換を行うものである。ルータ装置1は、LAN3に接続するLANインターフェース部11、WAN2に接続するWANインターフェース部12、入力したIPパケットが本ルータ装置1により処理すべきものかどうかを識別する入力処理部13、処理するパケットの内容の詳細を監視しアドレス変換テーブル18のエントリの参照、追加および内容変更を行うプロトコル・ポート番号判別部14、実際にパケットのアドレス変換を行うアドレス変換処理部15、パケットの適切なインターフェースへの転送を行うルーティング部16、アドレス変換テーブル18を監視し、一定時間参照のないエントリを削除するタイマ管理部17により構成される。アドレス変換テーブル18は、ルータ装置1のメモリ内部に確保され、アドレス変換処理の内容を記述したエントリを集積したものである。

【0023】ここで、図2を用いて従来のアドレス変換テーブルのエントリの構造と本実施の形態におけるアドレス変換テーブル18のエントリの構造の相違について説明する。図2(a)は従来のアドレス変換テーブルの構造であるが、アドレス変換処理に必要な情報がすべて含まれるエントリが新規の通信コネクションが生じる毎に生成される。図2(b)は本実施の形態におけるアドレス変換テーブル18の構造であるが、エントリがパケットの送信元、宛先部分(IPレベル)と、その上位のプロトコルに関する部分(上位層レベル)とに階層化されている。また、この内で複数のエントリによって1つの通信セッションを構成するエントリが関連付けられている。

【0024】図3は本実施の形態のルータ装置1によるアドレス変換処理の流れを示すフローチャート、図4は本実施の形態のルータ装置1によるアドレス変換エントリのグループ化とエントリの生存時間の同期についての説明図である。

【0025】図4において、3aはLAN3に接続されたPC、2aはWAN2上の端末であり、PC3a、ルータ装置1、端末2aのIPアドレスをそれぞれA、B、Cとする。PC3aから端末2aに通信をする度に、図3に示す手順によってルータ装置1のアドレス変換テーブル18にエントリが追加されるが、エントリ新規作成のたびに図1のプロトコル・ポート番号判別部14が既存のアドレス変換エントリと関連付けられるものかどうか判定し、図4に示すアドレス変換テーブル18のようにFTP制御コネクション(TCP21番)とFTPデータコネクション(TCP20番)エントリが関連付けられる。関連付けられたエントリの生存時間は同期されるため、従来の技術の図9において説明したようなFTP通信のアドレス変換エントリの不正削除を防ぐことができる。

【0026】(実施の形態2)以下、本発明の第2実施の形態について、図5を参照しながら説明する。第2実施の形態のルータ装置1におけるアドレス変換処理の概要は、図1～図3で示したところと同様なので説明を省略する。第2実施の形態と従来の技術との相違点は、アドレス変換エントリのグループ化を行い、生存時間の同期などの管理を一括で行うところにある。

【0027】図5は第2実施の形態におけるルータ装置1のアドレス変換テーブル18の構成を示す図である。ルータ装置1をパケットが通過する際、図1のプロトコル・ポート番号判別部14によりパケットは検査され、上位プロトコル、宛先ポート番号などから、図5に示すようにエントリはグループ化され、エントリ中の生存時間はグループ内のエントリで統一され、生存時間管理などの処理が一括化される。

【0028】(実施の形態3)以下、本発明の第3実施の形態について、図6を参照しながら説明する。第3実

施の形態のルータ装置1におけるアドレス変換処理の概要は、図1～図3で示したところと同様なので説明を省略する。第3実施の形態と従来の技術との相違点は、通信プロトコルの種別、状態によってアドレス変換エントリ生存時間を最適化するところにある。

【0029】図6は第3実施の形態におけるルータ装置1によるアドレス変換エントリの生存時間の設定例を示す図である。例えば、IPの上位層のプロトコルについて、通信持続性が低い順番に、ICMP、UDP、TCPの順に生存時間の値を上げていく。また、その中でもコネクション型通信プロトコルであるTCPについては、その上で利用されるプロトコルによって、TelnetやFTPなどの通信の持続性が高いプロトコルと、POP3といった通信の持続性が低いプロトコルとでアドレス変換エントリ新規作成時にアドレス変換エントリ生存時間に高低をつける。

【0030】(実施の形態4)以下、本発明の第4実施の形態について、図7を参照しながら説明する。

【0031】図7は第4実施の形態におけるネットワーク構成を示す図である。第4実施の形態のルータ装置1におけるアドレス変換処理の概要は、図1～図3で示したところと同様なので説明を省略する。第4実施の形態と従来の技術との相違点は、接続先のネットワーク毎にアドレス変換エントリ生存時間を変更することにある。

【0032】図7において、2bはインターネット、2c、2dはPC3aの通信先となるネットワークである。ルータ装置1に予め信頼性の高いネットワークのIPアドレスを指定できるようにする。ネットワーク2cは登録されたネットワークである。PC3aから外部ネットワークに通信を行う場合、ルータ装置1にアドレス変換エントリが生成されるが、それがルータ装置1に登録済のネットワーク2cである場合、他の相手先に接続した場合よりも長いエントリ生存時間を設定する。こうすることで、家庭内ネットワークから勤務先のネットワークにTelnetした場合などで、常に相手先と通信をしていなくても、アドレス変換エントリが削除される心配をする必要がなくなり、未知のネットワークに接続する場合にはエントリ生存時間を短くすることで、その相手先からの不正アクセスをされる危険性を減らすことができる。

【0033】(実施の形態5)第5実施の形態のルータ装置1におけるアドレス変換処理の概要は、図1～図3で示したところと同様なので説明を省略する。第5実施の形態と従来の技術との相違点は、通信プロトコル状態遷移に同期してアドレス変換エントリ生存時間を最適化するところにある。

【0034】ルータ装置1内のアドレス変換テーブル18のエントリを図1のプロトコル・ポート番号判別部14が参照する場合、上位プロトコルがTCPのパケットについては、TCPの通信内容を監視し、FINメッセージ

ージが通過する場合は、該当するエントリの生存時間を短くし、RSTメッセージが通過する場合には、該当するエントリを削除するといったTCPの状態遷移に応じたエントリ生存時間管理を行う。

【0035】

【発明の効果】本発明によれば、アドレス変換機能のために通信セッションが不正に切断されることを防ぐことで適切な通信接続性を確保し、効率的にメモリを利用して高速のアドレス変換エントリ管理方式を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1実施の形態におけるネットワーク構成を示す図

【図2】(a)従来のアドレス変換テーブルの構造を示す図

(b)本実施の形態におけるアドレス変換テーブルの構造を示す図

【図3】本実施の形態のルータ装置によるアドレス変換処理の流れを示すフローチャート

【図4】本実施の形態のルータ装置によるアドレス変換エントリのグループ化とエントリの生存時間の同期についての説明図

【図5】第2実施の形態におけるルータ装置のアドレス変換テーブルの構成を示す図

【図6】第3実施の形態におけるルータ装置1によるアドレス変換エントリの生存時間の設定例を示す図

【図7】第4実施の形態におけるネットワーク構成を示す図

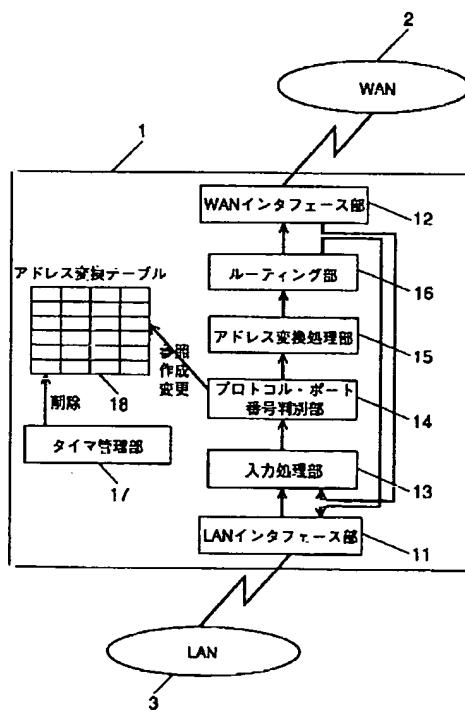
【図8】従来のネットワーク構成とアドレス変換処理の概要を示す図

【図9】従来の方式によるアドレス変換処理によって起こりうる問題点を示す説明図

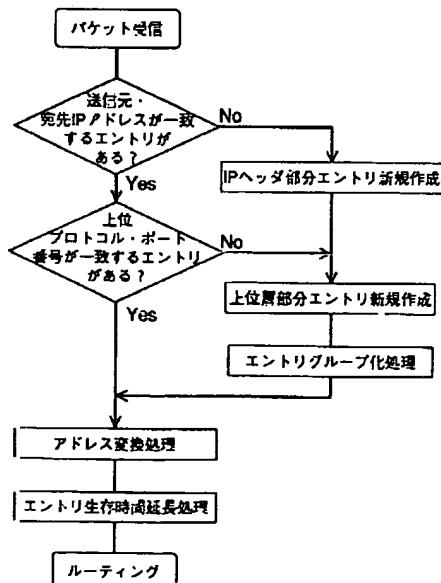
【符号の説明】

- 1 ルータ装置
- 2 WAN
- 2a 端末
- 2b インターネット
- 2c, 2d ネットワーク
- 3 LAN
- 3a PC
- 11 LANインターフェース部
- 12 WANインターフェース部
- 13 入力処理部
- 14 プロトコル・ポート番号判別部
- 15 アドレス変換処理部
- 16 ルーティング部
- 17 タイマ管理部
- 18 アドレス変換テーブル

【図1】

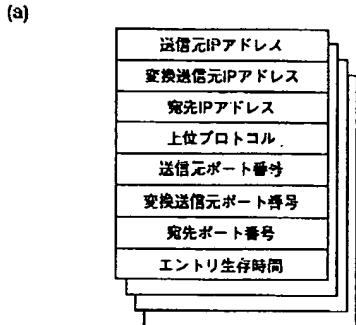


【図3】

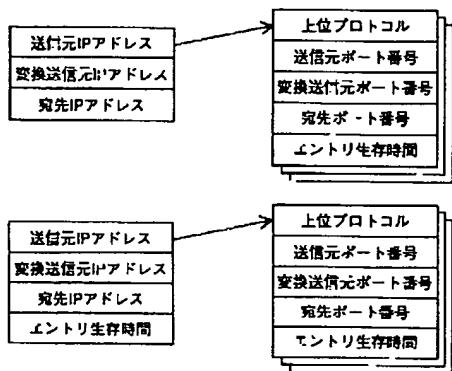


(6) 002-354048 (P2002-354048A)

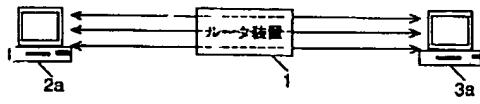
【図2】



(b)



【図4】



ルータ基盤1のアドレス変換テーブル18

送信元-A	プロトコル	送信元	宛先	生存時間
変更後=B	TCP	4000	20	300
	TCP	4001	21	300

関連付け

【図6】

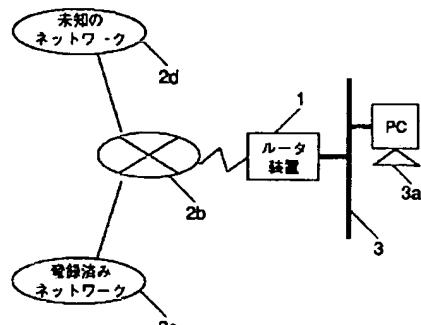
上位プロトコル	ポート番号	生存時間
ICMP	—	30秒
UDP	—	5分
TCP	110 (POP3)	10分
	25 (SMTP)	
	:	:
	21 (FTP)	20分
	20 (FTP)	
	23 (Telnet)	30分

【図5】

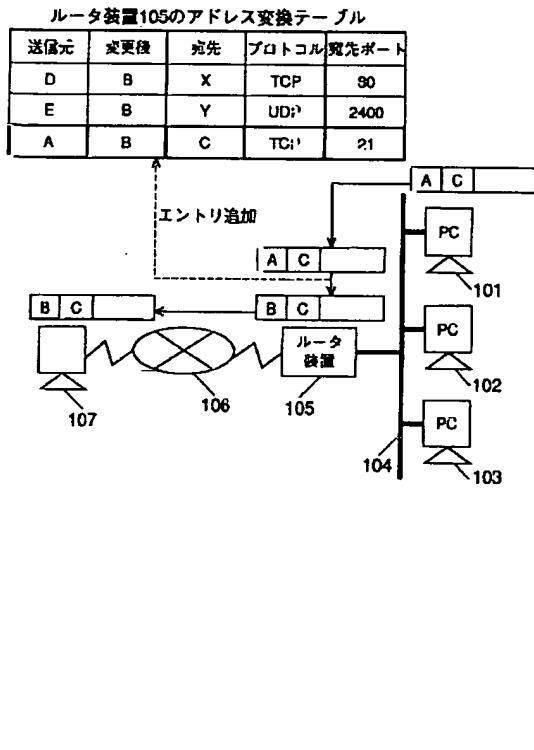
送信元IPアドレス	プロトコル	送信元	宛先	生存時間
変更後IPアドレス	TCP	4000	20	300
	TCP	4001	21	
	TCP	4002	80	60
	TCP	4003	80	
	TCP	4004	80	
	ICMP	—	—	15
	UDP	4010	161	150
	UDP	4011	162	

FTP グループ
HTTP グループ
SNMP グループ

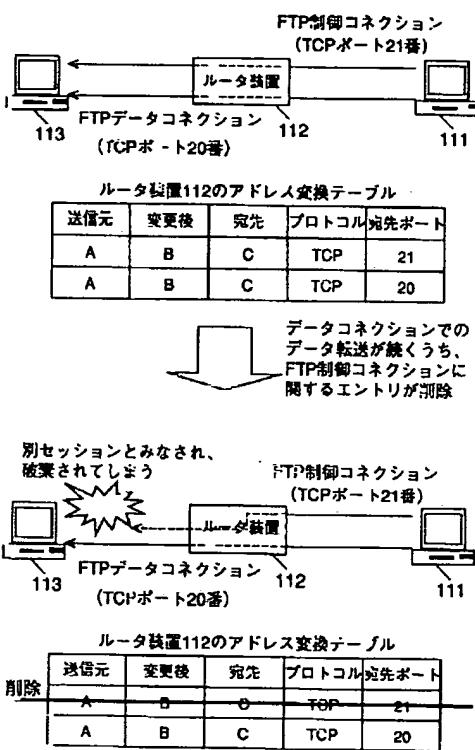
【図7】



【図8】



【図9】



フロントページの続き

F ターム(参考) 5K030 HC01 HC14 HD03 HD06 HD09
KA05 LB05
5K033 CB09 DA06 DB18 EC04